De factoribus numerorum compositorum dignoscendis

Disquisitio Academica,

cujus partem primam,

adnuente amplissima Fac. Philos.

Præside

CAROLO JOH. Ds HILL,

Math. Prof. Reg. & Ord.

pro summis in philosophia capessendis honoribus

exhibet

CAROLUS FREDRICUS LILJEVALCH,

Scanus.

In Academia Carolina Die II Junii MDCCCXXXVIII.

LUNDÆ,

TYPIS EXCUDIT C. FR. BERLING,

UNIVERSITATIS TYPOGRAPHUS.

MDCCCXXXVIII.

De factoribus numerorum compositorum disquirendis.

Ad libros*) quos de schemate residuorum, quorum ope numerus datus compositus num [illegible] primum sit an factorum agnoscat, nec ne. Quamquam illis demonstrationes brevitatis causa omittendas diximus, tamen ad numeros auxiliares schematum [illegible] quisque modo facile sibi explicet. Plurimi forsan praeceptores jam ex regulis illuc descriptis [illegible] eliciuerunt. Res enim prima elementa tangit et multum miramur, ejusmodi regulas jam antiquitus [illegible] neglecta fuerunt.

Vulgo rem ita proposuerunt, ut numerum datum N sub sua forma decadica explicatum ($N = a_0 + 10a_1 + 100a_2 + \ldots$) per numerum primum [illegible]. Sic $p = 7$ [illegible], ut ex residuo ($R = a_0 + 3a_1 + 2a_2 + \ldots$ quia $p = 7$) regulam eliceerint. Id quod cel. Gauss (Demonstrat. Rechenk. p. 409) ad numerum 7 agnoscendum praecipit. Nos vero numeros in isto residuo minimos eligimus, indeque regulas selectas primi generis ($\ldots$) expressas componimus. Ex. gr. ad divisorem $p = 7$ terminum $3a_1$

*) Crelle Journ. für reine und angewandte Math. T. XI. p. 251. XII. p. 355.

De factoribus numerorum dignoscendis.

Alibi *) regulas et schemata dedimus, quorum ope numerus datus comprobari poterit, num certum numerum primum ut factorum agnoscat, nec ne. Quamquam illibi demonstrationes brevitatis causa omittendas diximus, tamen ad numeros auxiliares schematum inveniendos nonnullæ proponendæ sunt veritates, quas suo quisque modo fusius sibi explicet. Plurimi forsan præceptores jam ex regulis illibi descriptis demonstrationes elicuerunt. Res enim prima elementa tangit; et multum miramur, ejusmodi regulas jam antiquitus propositas haud fuisse, — at elementa jam diu neglecta fuerunt.

Vulgo rem ita proposuerunt, ut numerum datum N sub sua forma decadica explicitum ($N = a_0 + 10\,a + 100\,a + ..$) per numerum primum suppositum (ex. gr. $p = 7$) diviserint, et ex residuo ($R = a_0 + 3\,a_1 + 2\,a_2 + \ldots$, cum $p = 7$) regulam elicuerint. Id quod cel. Clausberg (Demonstrat. Rechenk. p. 409) ad numerum 7 agnoscendum præcipit. Nos vero numeros in isto residuo minimos eligimus, indeque regulas schemate primi generis $\left(\overset{\pm\nu}{a\cdot}\right)$ expressas componimus. Ex. gr. ad divisorem $p = 7$ terminum $2\,a_2$

*) Crelle Journ. für reine und angewandte Math. T. XI. p. 251. XII. p. 355.

in residuo R consideramus, et inde, cum $2 \underset{7}{\equiv} 100$ sit, numerum N sub forma centesimali $= A_0 + 100 A_1 + 100^2 A_2 +$, (positis sc. $a_0 + 10 a_1 = A_0$, etc.), considerandum arguimus. Ex hac vero observatione doctor quisque regulas $\left(\begin{smallmatrix} \pm\nu \\ a\,. \end{smallmatrix}\right)$ et facile eliciet et veras juveni perspicue demonstret.

Quod vero ad Schema alterum $\left(\begin{smallmatrix} \nu\pm \\ .\,\alpha \end{smallmatrix}\right)$ attinet, in casibus specialibus æque elementarie explicari potest. Ex. gr. hoc $(\overline{!\,2})$ ad $p = 7$ inde, quod $3 . 7 = 21$ sit, ita dilucidatur: sit ex. gr. hic $N = 651$, et supponatur N esse multiplum ipsius 7, et tollatur ultima nota 1, residuumque 65 tum simul cum 2 minuendum erit $(65 - 2 = 63)$, ut et ipsum multiplum ipsius 7 sit, hoc enim idem valet, ac si $21\ (= 3 . 7)$ subtrahatur et residuum per 10 dividatur. Nempe $651 - 21 = 630$ & $630 : 10 = 63$. Simile argumentum vero valet, si N non multiplum supponitur. Sit ex. gr. $N = 958$, et ultima nota expellenda; id quod tuto effici nequit, nisi, ultima 8 demta, et a reliquis 95 dematur $8 . 2$, ut ita ab integro 958 demtum sit $8 . 20 + 8 = 8 . 21 = 8 . 3 . 7$, i. e. multiplum ipsius 7. Et sic in reliquis.

Schema vero tertii generis $\left(\begin{smallmatrix} \pm\nu \\ \beta\cdot\,.\,\alpha \end{smallmatrix}\right)$ brevissime ex regulis numerorum congruentium dilucidatur. Majoris vero commoditatis caussa id, quod cel. Gauss per "$a \equiv$ b, modulo c" significat, breviter per "$a \underset{c}{\equiv} b$," vel simplicius per "$a \underset{c}{\backsim} b$" aut "$a \underset{c}{\backsim} b$" indicamus, vel si mavis per hoc "$a \backsim b \; 7 \; c$",*) (ubi $\backsim$ antiquitus similitudinis est signum, et 7 multiplicitatis nonnullis usitatum. Signum vero $=$ identitati reservamus). His vero positis, sequentia facile demonstramus *theoremata:*

---

*) Hæc signa vindicata videas in Skandia. Band. II. H. 1. pag. 159.

1) *Si fuerint α et p numeri inter se incompositi, et præterea primum $10^n\alpha - \beta$ atque $\alpha a + \beta b$ multipla ipsius p; erit et $a + 10^n b$ multiplum ipsius p.*

Quoniam enim $10^n\alpha - \beta \underset{p}{\backsim} o$; atque $\alpha a + \beta b \underset{p}{\backsim} o$, erit $\beta \underset{p}{\backsim} 10^n\alpha$, ideoque $\beta b \underset{p}{\backsim} 10^n\alpha b$, atque $10^n\alpha b + \alpha a \underset{p}{\backsim} \alpha a + \beta b \underset{p}{\backsim} o$, seu $\alpha(10^n b + a) \underset{p}{\backsim} o$, et igitur, cum α et p inter se primi sint, $10^n b + a \underset{p}{\backsim} o$. Q. E. D.

2) *Sin vero deinde fuerit quidem $10^n\alpha - \beta$ multiplum ipsius p, $a\alpha + \beta b$ vero non item, neque erit $a + 10^n b$ multiplum ipsius p.*

Tum enim erit equidem ex modo demonstratis $\beta b \underset{p}{\backsim} 10^n\alpha b$, et $10^n\alpha b + \alpha a \underset{p}{\backsim} \alpha a + b\beta$; quoniam vero $\alpha a + b\beta$ secundum p cum nihilo haud congruat, neque $10^n\alpha b + \alpha a$, nec igitur $10^n b + a$, factore α sublato, cum o congruet. Q. E. D.

Hinc sequitur, si datus fuerit numerus $N = a + 10^n b$, eique factorem inesse aliquem p suspicaris, cujus multiplum aliquod formæ $10^n\alpha - \beta$ noveris, rem facile dijudicabis considerando numerum minorem N', ex formula $a\alpha + b\beta$ computatum: utrumque enim (N et N') ad divisorem p, ex iis, quæ modo demonstrata sunt, æque se habebunt: si enim N' multiplum ipsius p fuerit, etiam N erit; sin minus, neque N per p exacte dividetur. At Schema nostrum tertii generis $\binom{+\,n}{\beta\,.\,\alpha}$ hujusmodi regulam indicat, ut $\binom{+\,n}{\beta\,.\,\alpha}.N$ seu $\binom{+\,n}{\beta\,.\,\alpha}.(10^n b + a) = \beta b + a\alpha = N'$ suppeditet, ideoque hoc schema $\binom{+\,n}{\beta\,.\,\alpha}$ ipsiusque regula ad factorem p, qui pars aliquota ipsius $10^n\alpha - \beta$ est, in numero N præsentem vel

absentem agnoscendum juvat. Sin vero fuerit $10^n\alpha - \beta = p.p.'p.''..$, eædem regulæ ad quemcunque numerum p', p'', ad α primum, æque quadrant, sicuti jam antea innuimus. Patet vero, easdem demonstrationes æque valere, si loco ipsius β ponatur $-\beta$; ideoque

3) *Si fuerint α et p invicem primi, et $10^n\alpha + \beta$ multiplum ipsius p; erit $a + 10^n b$ multiplum aut non multiplum ipsius p, prout $\alpha a - \beta b$ multiplum vel non multiplum ejusdem p fuerit.*

Inde vero et itidem consequitur, si fuerit $10^n\alpha + \beta = p.p.'p''..$ schematis $\left(\begin{smallmatrix} -n \\ \beta.\alpha \end{smallmatrix}\right)$ regulas ad quemvis divisorum $p, p,' p''...$ ad α primum, æque pertinere.

Præterea, cum in his demonstrationibus nullam vim ei rei tribuimus, quod 10 decem valeat, per 10 basin numerandi quamvis seu numerum quemcunque q intelligere licet, ideoque universim hæc valet *propositio.*

4) *Si fuerint α et p inter se primi, et $q.^n\alpha \pm \beta$ multiplum ipsius p; habebit numerus $(N=)$ $a + q^n b$ se ad divisorem p eundem in modum ac numerus alius $(N'=)$ $a\alpha \mp b\beta$,* ut scilicet per p exacte (N) dividatur, cum hic (N') dividitur, et residuum relinquat, cum hic relinquit; regulæ vero et conversæ valent.

Nempe si fuerit equidem $\alpha q^n \underset{p}{\backsim} \mp\beta$, et $a + q^n b \underset{p}{\backsim} o$ vel non $\underset{p}{\backsim} o$, erit $\mp\beta b \underset{p}{\backsim} \alpha q^n b$, et $a\alpha \mp \beta b \underset{p}{\backsim} a\alpha + \alpha q.^n b = \alpha.(a + q^n b) \underset{p}{\backsim} o$ vel non $\underset{p}{\backsim} o$. — Quæ igitur jam allata sunt, vim regularum nostrarum non modo tertii generis, seu ad Schema $\left(\begin{smallmatrix} \pm\nu \\ \beta.\alpha \end{smallmatrix}\right)$ pertinentium, sed etiam primi et secundi seu schematum $\left(\begin{smallmatrix} \pm\varkappa \\ a. \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} \nu\pm \\ .\alpha \end{smallmatrix}\right)$, cum hæc, ut olim innuimus, istius nonnisi casus speciales sint, et corroborant et eo extendunt, ut non modo in vulgari systemate

numerandi decadico, sed etiam in alio quocunque, cujus basis numerus est quivis q, æque valeant, dummodo numeri auxiliares α, β, ν, ad suum quemvis numerum exprobandum p rite accommodentur.

De his vero numeris auxiliaribus inveniendis jam agitur. Prævie tamen problema invertamus, et ad numeros α, β, ν utcunque electos divisorem idoneum p perquiramus. Patet vero ex jam dictis et comprobatis, hunc numerum non nisi aliquem factorum ipsius $10^\nu\alpha \pm \beta$ fore, eumque ab α diversum, ideoque schema $\left(\begin{smallmatrix}+\nu \\ \beta.\alpha\end{smallmatrix}\right)$ ad factorem quemvis numeri $10^\nu\alpha - \beta$, et $\left(\begin{smallmatrix}-\nu \\ \beta.\alpha\end{smallmatrix}\right)$ ad hujus $10^\nu\alpha + \beta$ factorem, ad α primum, pertinere.

Invenitur igitur p, numerum $10^\nu\alpha \pm \beta$ in factores (simplices vel compositos) resolvendo. Quam minimi vero sumendi sunt α et β, ut eo computus simplicior evadat.

1) Ponatur igitur primum $\beta = o$ et $\alpha = 1$, atque $10 = 2.5$, eritque $10^\nu = 2^\nu.5^\nu$, ideoque regula pro factoribus 2^ν vel 5^ν agnoscendis hæc erit notissima: "Numerus $(N=)$ $a + 10^\nu b$ per 2^ν vel 5^ν dividitur, cnm a dividitur," quam, si lubet, igitur per schema $\left(\begin{smallmatrix}\pm\nu \\ o.1\end{smallmatrix}\right)$ vel $\left(\begin{smallmatrix}+\nu \\ o\,.\end{smallmatrix}\right)$ indicare licet.

Quoniam vero hanc rem attigimus, speciales quasdam regulas ad *potentias ipsorum* 2 *et* 5 in numero composito recognoscendas obiter proponamus. Ope regularum $\left(\begin{smallmatrix}+I \\ o\,.\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}+II \\ o\,.\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}+III \\ o\,.\end{smallmatrix}\right)$ facile cognoscuntur 5, 5^2 et 5^3; quæ si igitur præsentiam potestatis tertiæ (5^3) arguerent, attioresque (5^4&c.) suspicarentur, numerum datum compositum in 1024 $(= 2^{10})$ ducas, numerusque dextrarum notarum zeroticarum producti exponentem subministrabit, si < 10 fuerit; sin minus, iterum similiter multiplices.

Ex. gr. $N = 9375$; Resol. $N.2^{10} = \left\{\begin{array}{r} 9375 \\ 18750 \\ 37500 \end{array}\right\} = 9600000$;

quare $N = p.5^5$ et $p = 96 : 2^5 = 3$. — Hoc modo igitur quæcunque *ipsius* 5 *potentia* cito detegitur; *ipsius vero* 2 *ita*: —

Sit $N = a + 10.a_1 + 100.a_2 + 1000.a_3 + \ldots$ &

1) per 2^2 divisibilis, eritque, ex schemate $\left(\begin{smallmatrix} & +II \\ o & . \end{smallmatrix}\right)$, etiam $a + 10a_1$ per 2^2 divisibilis, seu $a \underset{2}{\backsim} o$, et $a + 10a_1 \underset{4}{\backsim} o$. Sit igitur $a = 2\alpha$, eritque $2\alpha + 10a_1 \underset{4}{\backsim} o$ seu $2\alpha + 2a_1 \underset{4}{\backsim} o$, ideoque $\alpha + a_1 \underset{2}{\backsim} o$; ponatur igitur $\alpha + a_1 = 2\beta$, eritque, si $N \underset{4}{\backsim} o$, tum $\frac{a}{2} = \alpha$, tum $\frac{1}{2}(\alpha + a_1) = \beta =$ numerus integer.

2) Sit ulterius $N \underset{8}{\backsim} o$, seu $(o\,\overset{III}{.})$ $N = a + 10a_1 + 100a_2 \underset{8}{\backsim} o$, seu $a + 2a_1 + 4a_2 \underset{8}{\backsim} o$, seu, positis $\alpha = \frac{1}{2}a$, & $\beta = \frac{1}{2}(\alpha + a_1)$, $2.2\beta + 4a_2 \underset{8}{\backsim} o$. ideoque $\beta + a_2 \underset{2}{\backsim} o$. Quivis igitur numerus N (ex. gr. 256), num per 2, vel 4, vel 8, dividatur, ita rimandus:

Dimidium ultimæ notæ addatur penultimæ, quod idem, si succedit, iteretur bis vel ter, præcedente scilicet deleta.

$$\begin{array}{rl}
 & 25|6 \\
\alpha = & \underline{+3|} = \frac{6}{2} \\
 & 2|8 \\
\beta = & \underline{+4|} = \frac{8}{2}\ \left(= \frac{5+3}{2}\right) \\
 & 0|6 \\
 & \underline{+3|} = \frac{6}{2}\ \left(= \frac{2+4}{2}\right). \\
 & 3
\end{array}$$

256 igitur saltim per 2.2.2 dividitur.

3) Deinde sit $N \underset{16}{\backsim} o$, ideoque

$\left(\binom{+IV}{o\,.}\; N = \right) a + a_1 . 10 + a_2 . 10^2 + a_3 . 10^3 \underset{16}{\backsim} o$ seu $a + 10a_1 + 4a_2 + 8a_3 \underset{16}{\backsim} o$. Est enim $100 \underset{16}{\backsim} 4$, & igitur $1000 \underset{16}{\backsim} 40 \underset{16}{\backsim} 8$. At $a = 2\,\alpha$, $\alpha + a_1 = 2\beta$ (ut in 2).), $a + 10a_1 = 2\alpha + 2a_1 + 8a_1 = 4\beta + 8a_1$, et $N \underset{2^3}{\backsim} o$, ideoque $4\beta + 4a_2 \underset{8}{\backsim} o$, seu $\beta + a_2 \underset{2}{\backsim} o$. Sit igitur $\beta + a_2 = 2\gamma$, eritque $a + 10\,a_1 + 4\,a_2 = 4\beta + 4\,a_2 + 8\,a_1 = 8\,\gamma + 8\,a_1$, et igitur $8\gamma + 8a_1 + 8a_3 \underset{16}{\backsim} o$, ex quo sequitur $\gamma + a_1 + a_3 \underset{2}{\backsim} o$. Poni igitur potest $\gamma + a_1 + a_3 = 2\,.\,\delta$, exsistente δ numero integro. Ideoque si fuerit $N 7\, 16$, erit $a = 2\alpha$, $\alpha + a_1 = 2\beta$, $\beta + a_2 = 2\,.\,\gamma$ et $\gamma + a_1 + a_3 = 2\delta$.

Ex. $N = \overset{a_2 a_1 a}{256}$, quo casu $\alpha = 3$, $\beta = 4$, $\gamma = 3$, $\delta = 4 \left(= \frac{3+5+0}{2}\right)$.

4) Sit ulterius $N \underset{32}{\backsim} o$, ideoque et $N \underset{16}{\backsim} o$, et ex modo demonstratis, $\gamma + a_1 + a_3 = 2\delta$, atque $a + 10\,a_1 + 4\,a_2 = 8\,(\gamma + a_1)$. Quoniam vero $N \underset{2^5}{\backsim} o$, ideoque schema $\binom{+V}{o\,.}$ valet, et suppeditat $\binom{+V}{o\,.}$ $N = a + 10\,a_1 + 10^2 a_2 + 10^3 a_3 + 10^4 a_4 \underset{32}{\backsim} o$, seu $a_0 + 10a_1 + 4a_2 + 8a_3 + 16a_4 \underset{32}{\backsim} o$, erit $8\,(\gamma + a_1) + 8a_3 + 16a_4 \underset{32}{\backsim} o$, seu $16\,(\delta + a_4) \underset{32}{\backsim} o$, ideoque $\delta + a_4 \underset{2}{\backsim} o$. "Dicta (ad 2) igitur illa dimidii ultimarum additione ter instituta, tum quotus ille tertius (γ) tum nota secunda (a_1) quartæ (a_3) addenda sunt, et summa par erit, si divisio per 16 succedat; deinde vero istius summæ dimidium (δ) quintæ (a_4) additum par erit, si 32 est justus divisor."

Ex. gr. $N = \overset{a_4}{7}\overset{a_3}{0}\overset{a_2}{6}\overset{a_1}{1}\,4|\overset{a}{4}$

$$\begin{array}{l}
\alpha = \quad +\,2| \ (= \tfrac{1}{2}\cdot 4)\\
\beta = \ +\,3|6 \ (= a_1 + \alpha = 2\beta), \text{ (seu } 3 = \tfrac{1}{2}\cdot(4+2)\\
\gamma = +\,2|4 = (= \beta + a_2 = 2\gamma), \text{ (seu } 2 = \tfrac{1}{2}\cdot(1+3).\\
a_1 = +\,4|\\
\delta = +\,6|12 = 2.6 \ (= \overset{a_3}{6} + \overset{\gamma}{2} + \overset{a_1}{4}) = 2\delta.
\end{array}$$

Ergo $a_4 + \delta = o + 6 = 2.3$, ideoque N 7 32.

De his divisoribus (16, 32) et hæc regula valet:

"Quarta pars zyphræ centesimalis ultimæ (seu duarum ultimarum zifrarum decadicarum) penultimis tribus addatur, summæque iterum quarta pars perquiratur, num integra sit."

Ex. gr. $N = 7061|44$

$$\begin{array}{l}
\quad +\,11| = \tfrac{1}{4}\,(44)\\
\quad 7|072 \ (= 4.018)
\end{array}$$

"vel etiam hæc summa (7072) secundum 4 vel 8 comprobetur."

$$\begin{array}{lll}
707|2 & \qquad & \text{Ex. } 195|36\\
+\,1| = \tfrac{2}{2} & & +\,9|\cdot\cdot 4\\
70|8 & & 20|4\\
+\,4| = \tfrac{8}{2} & & 2| = \tfrac{4}{2}\\
7|4 & & 2|2\\
2| = \tfrac{4}{2} & & 1| = \tfrac{2}{2}\\
9 & & 3
\end{array}$$

Hic N igitur per $4.2.2.2 = 2^5$ dividitur, sed 19536 tantum per 16.

Sit enim universim $N = A + 100\,A_1$ et $p = 16$ vel 32, eritque $N \underset{p}{\backsim} A + 4A_1$, ideoque si $N \underset{p}{\backsim} o$, et ita $N \underset{4}{\backsim} o$, atque $A \underset{4}{\backsim} o$, seu $A = 4B$, et tandem $4(B + A_1) \underset{p}{\backsim} N \underset{p}{\backsim} o$, ideoque $B + A_1 \underset{\frac{1}{4}p}{\backsim} o$, i. e. $(A_1 + \tfrac{1}{4}A) \underset{4}{\backsim} o$ si $N \underset{16}{\backsim} o$, atque $(A_1 + \tfrac{1}{4}A) \underset{8}{\backsim} o$, si $N \underset{32}{\backsim} o$: Quod ipsam regulam constituit.